REMARKS

This application has been carefully reviewed in light of the Office Action dated December 18, 2002. Claims 1 to 3, 6, 7, 10 to 14, 18 to 20 and 22 remain in the application, with Claims 4, 5, 8 and 9 having been canceled, and Claims 1, 10, 12, 14, 18, 20 and 22 having been amended. Claims 1, 10, 14, 18, 20 and 22 are the independent claims herein. Reconsideration and further examination are respectfully requested.

Claims 1 to 6, 8, 10 to 14, 18, 20 and 22 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,535,277 (Shibata) in view of U.S. Patent No. 5,870,468 (Harrison), and Claims 7, 9 and 19 were rejected under § 103(a) over Shibata in view of Harrison and further in view of portions of a book entitled "Applied Cryptography" by Bruce Schneier (hereinafter referred to as "Schneier"). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns encryption of digital information. According to the invention, an encryption key stored in an external source is read and stored in a storage means to execute an encryption process. The external encryption key is used to encrypt either digital information or an internal encryption key that has been used to encrypt the digital information. After completion of the encryption process, either the encrypted digital information, or both the encrypted digital information and the encrypted internal encryption key are output. Then, corresponding to the output of the encrypted digital information and, if applicable, the encrypted internal encryption key, the external encryption key stored in the storage means is erased from the storage means. As a result, erasing of the external encryption key significantly reduces the likelihood that a hacker will

be able to obtain the external encryption key from the storage means and so as to be able to decrypt the digital information.

With specific reference to the claims, amended independent Claim 1 is an image input apparatus comprising reading means for reading an encryption key stored in an external source, storage means for storing the encryption key to execute an encryption process; encryption means for encrypting digital information by using the encryption key stored in the storage means; output means for outputting the encrypted digital information after completion of the encryption by the encryption means, and erasing means for erasing the encryption key stored in the storage means corresponding to the outputting of the encrypted digital information.

Amended independent Claims 10 and 14 are method and computer program claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 is an image input apparatus comprising information encryption means for encrypting digital information by using an internal encryption key, obtaining means for obtaining an external encryption key stored in an external source, storage means for storing the external encryption key to execute a key encryption process, key encryption means for encrypting the internal encryption key by using the external encryption key stored in the storage means, output means for outputting the encrypted digital information and the encrypted internal encryption key after completion of the key encryption by the key encryption means, and erasing means for erasing the external encryption key stored in the storage means corresponding to the outputting of the encrypted digital information and the encrypted internal encryption key.

Amended independent Claims 20 and 22 are method and computer program claims, respectively, that substantially correspond to Claim 18.

The applied art, alone or in combination, is not seen to disclose or to suggest the features of independent Claims 1, 10, 14, 18, 20 and 22. More particularly, the applied art is not seen to disclose or to suggest at least the feature of reading and storing in a storage means an external encryption key stored in an external source, and after completion of encrypting digital information using the external encryption key stored in the storage means and outputting of the encrypted digital information (Claims 1, 10 and 14), or after completion of encrypting an internal encryption key, that has been used to encrypt digital information, using the external encryption key, and outputting of the encrypted digital information and the encrypted internal encryption key (Claims 18, 20 and 22), erasing the external encryption key stored in the storage means corresponding with the outputting.

Shibata is seen to disclose that an encryption/decryption circuit 403 encrypts data using an encryption key maintained by the circuit. After encryption is completed, the encrypted data is transmitted over a phone line. In Shibata, a user can register (i.e., create), change and delete an encryption key by assigning a ten-digit number. The user performs these processes via an operation section 7. (See column 4, lines 48 to 51 and column 7, lines 39 to 45.) However, the encryption key used to encrypt the data in Shibata is maintained in the device (i.e., it is an internal key) and is not a key stored in and read from an external source. In this regard, the Office Action asserted at paragraph 2 on page 2 that a user registering (i.e., creating) an encryption key that is then maintained within the device

allegedly reads on an external source. However, the user merely inputs a code to create an encryption key, while the device itself then creates the encryption key and stores the key internally. The code input by the user is not an encryption key, but merely a code used to create the encryption key. Therefore, the user in Shibata does not correspond to reading an encryption key stored in an external source. Moreover, the Office Admits that Shibata fails to disclose erasing the encryption key when the encryption process is completed and therefore, Shibata cannot erase the external encryption key stored in a storage means corresponding with outputting of encrypted digital information.

Harrison is merely seen to disclose that files are encrypted with an encryption key and two scrambled versions of the encryption key are stored in the computer, one scrambled with a secret key and the other scrambled with a transform of the secret key. The unscrambled version of the encryption key is then erased from the computer's memory, but the scrambled versions of the encryption key remain in the computer. When a user enters the proper secret key, the scrambled versions are unscrambled and the encryption key is restored in the computer and used to decrypt any encrypted files. Thus, Harrison makes multiple versions (copies) of the encryption key and only erases one of those versions, with the other versions of the encryption key remaining in the computer, albeit in a scrambled format, which are later used to restore the encryption key. (See column 4, lines 30 to 47, and column 6, lines 43 to 52.) However, Harrison, like Shibata, is not seen to disclose that an external encryption key stored in an external source is read and stored in the device. Moreover, while Harrison erases encryption keys, Harrison is not seen to disclose or to suggest that after completion of encrypting digital

information using the external encryption key stored in the storage means and outputting of the encrypted digital information (Claims 1, 10 and 14), or after completion of encrypting an internal encryption key, that has been used to encrypt digital information, using the external encryption key, and outputting of the encrypted digital information and the encrypted internal encryption key (Claims 18, 20 and 22), the external encryption key stored in the storage means is erased corresponding with the outputting.

Schneier is not seen to add anything to overcome the deficiencies of Shibata and Harrison and is also not seen to disclose or to suggest at least the feature of reading and storing in a storage means an external encryption key stored in an external source, and after completion of encrypting digital information using the external encryption key stored in the storage means and outputting of the encrypted digital information (Claims 1, 10 and 14), or after completion of encrypting an internal encryption key, that has been used to encrypt digital information, using the external encryption key, and outputting of the encrypted digital information and the encrypted internal encryption key (Claims 18, 20 and 22), erasing the external encryption key stored in the storage means corresponding with the outputting.

In view of the foregoing deficiencies of the applied art, all of Claims 1 to 3, 6, 7, 10 to 14, 18 to 20 and 22 are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant

Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 59917 v 1